МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ В.Ф. УТКИНА»

Кафедра «Государственного, муниципального и корпоративного управления»

«СОГЛАСОВАНО»
Декан факультета ИЭ
_____ Горбова О.Ю.
«26» 06 2020 г.
Заведующий кафедрой ГМКУ
_____ Перфильев С.В.
«26» 06 2020 г.

«УТВЕРЖДАЮ»
Проректор по РОПиМД
_____ Корячко А.В.
«__» _____ 2020 г.

РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.08.01 «Информационная безопасность»

Направление подготовки – 38.03.04 Государственное и муниципальное управление

Профиль – Информационные технологии в государственном и муниципальном управлении

ОПОП академического бакалавриата
«Государственное и муниципальное управление»

Квалификация выпускника – бакалавр
Формы обучения – заочная

Рязань 2020 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования по направлению подготовки 38.03.04 «Государственное и муниципальное управление», утвержденным приказом Минобрнауки России № 1567 от 10.12.2014 г.

Разработчик

доцент кафедры АСУ / Челебаев С.В. /

(должность, кафедра) (подпись) (Расшифровка)

Заведующий кафедрой

АСУ / Холопов С.Ч. /

(кафедра) (подпись) (Расшифровка)

Рассмотрена и утверждена на заседании кафедры «25» 06 2020г., протокол № 10

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы бакалавриата

Рабочая программа по дисциплине «Информационная безопасность» составлена в соответствии с требованиями, установленными Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 38.03.04 «Государственное и муниципальное управление», утвержденным приказом Минобрнауки России № 1567 от 10.12.2014 г.

Программа предназначена для студентов, обучающихся по основной профессиональной образовательной программе (далее – ОПОП) «Государственное и муниципальное управление» реализуемой по направлению подготовки 38.03.04 «Государственное и муниципальное управление» (уровень бакалавриата).

Целью освоения дисциплины «Информационная безопасность» является ознакомление обучающихся с основными направлениями деятельности по обеспечению информационной безопасности, рассмотрение аспектов нормативно-правовой базы, регламентирующей данную деятельность, задач руководителей, специалистов по сохранности информационных ресурсов, средств и механизмов, в том числе аппаратно-программных, используемых для этих целей, и методов их применения.

Задачи освоения учебной дисциплины:

- сформировать общее представление об информационной безопасности как о состоянии защищенности информационного ресурса сложной системы, понимание необходимости системного подхода к практической реализации такого состояния;
- передать знания о порядке организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации;
- сформировать навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к дисциплинам по выбору Блока 1 (Б1.В.ДВ.08.01) учебного плана основной профессиональной образовательнойи программы (ОПОП). Дисциплина изучается на 4 курсе в 8 семестре по очной форме обучения и на 5-м курсе в 10-м семестре по заочной форме обучения.

Требования к входным знаниям, умениям и компетенциям студента, необходимые для изучения данной дисциплины, совпадают с выходными знаниями, умениями и компетенциями, полученными в ходе изучения следующих дисциплин предусмотренных учебным планом подготовки бакалавров: «Информационно-коммуникационные технологии в профессиональной сфере», «Web-программирование».

Теоретические знания и практические навыки в области информационной безопасности могут быть использованы в процессе выполнения и подготовке к защите выпускной квалификационной работы.

Перечень планируемых результатов обучения по дисциплине

Коды компетенций	*Содержание компетенций*	*Перечень планируемых результатов обучения по дисциплине*
ОПК-1	владением навыками поиска, анализа и использования нормативных и правовых документов в своей	Знать: законодательный уровень информационной безопасности. Уметь: применять объектно-ориентированный подход к рассмотрению защищаемых систем. Владеть: навыками использования нормативной

Коды компетенций	*Содержание компетенций*	*Перечень планируемых результатов обучения по дисциплине*
	профессиональной деятельности	документации информационной безопасности
ПК-8	способностью применять информационно-коммуникационные технологии в профессиональной деятельности с видением их взаимосвязей и перспектив использования	Знать: понятия информационной безопасности, основные составляющие информационной безопасности. Уметь: выбрать соответствующие информационные технологии обеспечения информационной безопасности. Владеть: навыками использования технологий информационной безопасности

4 Структура и содержание дисциплины

4.1 Объем дисциплины по семестрам (курсам) и видам занятий в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 2 зачетных единицы (72 часа).

Вид учебной работы	Всего часов
	Заочная форма
Общая трудоемкость дисциплины, в том числе:	**72**
Контактная работа обучающихся с преподавателем (всего), в том числе:	8,25
Лекции	4
Практические занятия	-
Лабораторные работы	4
Консультации	-
ИКР	0,25
Самостоятельная работа обучающихся (всего), в том числе:	63,75
Самостоятельные занятия	50
КоР	10
Контроль	3,75
Вид промежуточной аттестации обучающихся–Зачет	-

4.2. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

Заочная форма обучения

№п/п	Раздел дисциплины	Общая трудоемкость	Контактная работа				Самостоятельная работа
			Всего	Лекции	ПЗ (или С)	ЛР	
1	Понятие информационной безопасности. Основные составляющие	7	1	1	-	-	6
2	Объектно-ориентированный подход к рассмотрению защищаемых	7	1	1	-	-	6

	систем. Наиболее распространенные угрозы информационной безопасности и её составляющие						
3	Законодательный уровень информационной безопасности. Административный уровень информационной безопасности	7	1	1	-	-	6
4	Процедурный уровень информационной безопасности	7	1	1	-	-	6
5	Основные характеристики программно-технических мер. Идентификация и аутентификация	11	4	-	-	4	7
6	Протоколирование и аудит, шифрование, контроль целостности.	11	-	-	-	-	11
7	Экранирование, анализ защищенности	15	-	-	-	-	15
8	Обеспечение высокой доступности	7	-	-	-	-	7
	Всего	72	8	4	-	4	64

4.3 Содержание дисциплины

4.3.1 Лекционные занятия

№	Наименование раздела дисциплины	Содержание раздела	Трудоемкость (час)	Формируемые компетенции	Форма контроля
1	Понятие информационной безопасности. Основные составляющие	Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб. Доступность, целостность, конфиденциальность. Компьютерное преступление, жизненный цикл информационных систем.	2	ОПК-1	Зачет
2	Объектно-ориентированный подход к рассмотрению защищаемых систем. Наиболее распространенные угрозы	Сложные системы. Структурный подход. Объектно-ориентированный подход, класс, объект, метод объекта, инкапсуляция, наследование, полиморфизм, грань объекта, уровень детализации ИС, деление на субъекты и объекты,	2	ОПК-1	Зачет

	информационной безопасности и её составляющие	безопасность повторного использования объектов, учет семантики. Операционная система как сервис безопасности. Основные определения и критерии классификации угроз. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.			
3	Законодательный уровень информационной безопасности. Административный уровень информационной безопасности	Российское законодательство в области информационной безопасности. Зарубежное законодательство в области информационной безопасности. Стандарты и спецификации в области информационной безопасности. Основные понятия административного уровня, политика безопасности. Жизненный цикл информационной системы. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками	2	ОПК-1	Зачет
4	Процедурный уровень информационной безопасности	Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.	2	ОПК-1	Зачет
5	Основные характеристики программно-технических мер. Идентификация и аутентификация	Основные понятия программно-технического уровня. Архитектурная безопасность. Экранирование. Анализ защищённости. Отказоустойчивость. Безопасное восстановление. Основные понятия. Парольная аутентификация. Одноразовые пароли. Сервер аутентификации Kerberos. Идентификация/аутентификация с помощью биометрических	2	ОПК-1, ПК-8	Зачет

		данных. Управление доступом. Ролевое управление доступом.			
6	Протоколирование и аудит, шифрование, контроль целостности	Основные понятия. Активный аудит. Шифрование. Симметричный метод шифрования. Асимметричный метод шифрования. Секретный и открытый ключ. Криптография. Контроль целостности. Цифровые сертификаты. Электронная цифровая подпись.	2	ПК-8	Зачет
7	Экранирование, анализ защищенности	Основные понятия. Экранирование. Фильтрация. Межсетевые экраны. Классификация межсетевых экранов. Архитектурная безопасность. Транспортное экранирование. Анализ защищенности. База данных уязвимостей. Сетевой сканер. Антивирусная защита.	2	ПК-8	Зачет
8	Обеспечение высокой доступности	Эффективность услуг. Время недоступности. Основы мер обеспечения высокой доступности. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости. Обеспечение обслуживаемости. Туннелирование.	2	ПК-8	Зачет

4.3.2 Лабораторные работы

№ пп	**Тема лабораторной работы**	Раздел дисциплины	Трудоемкость, час	Форми-руемые компе-тенции	Формы контроля
1	Идентификация и аутентификация	5	4	ОПК-1	Зачет
2	Шифрование	6	4	ПК-8	Зачет
3	Криптография	6	4	ПК-8	Зачет
4	Экранирование	7	4	ПК-8	Зачет

4.3.3 Самостоятельная работа

Самостоятельная работа студентов по дисциплине «Информационная безопасность» предназначена для развития у обучающихся навыков целенаправленного самостоятельного приобретения новых знаний и умений.

Самостоятельная работа включает в себя следующие составляющие:

- изучение теоретического материала по конспектам лекций;

- самостоятельное изучение дополнительных информационных ресурсов по темам разделов дисциплины, приведенных в п. 6 «Учебно-методическое обеспечение дисциплины»;
- выполнение заданий текущего контроля успеваемости (подготовка к лабораторным работам и сдача лабораторных работ);
- выполнение заданий по лабораторным работам;
- итоговая аттестация по дисциплине (подготовка к зачету).

Подготовка к лабораторной работе предполагает изучение лекционного материала по теме лабораторной работы и разделов «Краткие теоретические сведения» в методических указаниях к лабораторным работам (теоретическая подготовка) и проведение предварительных расчетов, необходимых для успешного выполнения лабораторной работы.

№ п/п	Тематика самостоятельной работы	Трудоем-кость (час.)	Форми-руемые компе-тенции	Формы контроля
		заочная		
1	Подготовка по разделу 1 Понятие информационной безопасности. Основные составляющие [1, 2]	6	ОПК-1	зачет
2	Подготовка по разделу 2 Объектно-ориентированный подход к рассмотрению защищаемых систем. Наиболее распространенные угрозы информационной безопасности и её составляющие [2, 3]	6	ОПК-1	зачет
3	Подготовка по разделу 3 Законодательный уровень информационной безопасности. Административный уровень информационной безопасности [3, 4]	6	ОПК-1	зачет
4	Подготовка по разделу 4 Процедурный уровень информационной безопасности [4, 5]	6	ОПК-1	зачет
5	Подготовка по разделу 5 Основные характеристики программно-технических мер. Идентификация и аутентификация [5, 6]	7	ОПК-1, ПК-8	ЛР, зачет
6	Подготовка по разделу 6 Протоколирование и аудит, шифрование, контроль целостности [6, 7]	11	ПК-8	ЛР, зачет
7	Подготовка по разделу 7 Экранирование, анализ защищенности [7, 8]	15	ПК-8	ЛР, зачет
8	Подготовка по разделу 8 Обеспечение высокой доступности [7, 8]	7	ПК-8	зачет

5. Оценочные материалы для проведения промежуточной аттестации обучающихся по дисциплине

Ооценочные средств приведены в Приложении к рабочей программе дисциплины в документе «Оценочные материалы» по дисциплине «Фильтрационная обработка процессов в информационных системах».

6. Учебно-методическое обеспечения дисциплины

6.1. Основная учебная литература:

1. Фомин Д.В. Информационная безопасность [Электронный ресурс]: учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения/ Фомин Д.В.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 54 c.— Режим доступа: http://www.iprbookshop.ru/77320.html.— ЭБС «IPRbooks»

2. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 c.— Режим доступа: http://www.iprbookshop.ru/33430.html.— ЭБС «IPRbooks»

3. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]/ Фаронов А.Е.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 154 c.— Режим доступа: http://www.iprbookshop.ru/52160.html.— ЭБС «IPRbooks»

4. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 c.— Режим доступа: http://www.iprbookshop.ru/52209.html.— ЭБС «IPRbooks»

5. Авдошин С.М. Технологии и продукты Microsoft в обеспечении информационной безопасности [Электронный ресурс]/ Авдошин С.М., Савельева А.А., Сердюк В.А.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017.— 412 c.— Режим доступа: http://www.iprbookshop.ru/72341.html.— ЭБС «IPRbooks»

6. Дождиков В.Г. Краткий энциклопедический словарь по информационной безопасности [Электронный ресурс]/ Дождиков В.Г., Салтан М.И.— Электрон. текстовые данные.— М.: Энергия, 2010.— 239 c.— Режим доступа: http://www.iprbookshop.ru/5729.html.— ЭБС «IPRbooks»

7. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 c.— Режим доступа: http://www.iprbookshop.ru/10677.html.— ЭБС «IPRbooks»

8. Спицын В.Г. Информационная безопасность вычислительной техники [Электронный ресурс]: учебное пособие / Спицын В.Г.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011.— 148 c.— Режим доступа: http://www.iprbookshop.ru/13936.html.— ЭБС «IPRbooks»

6.2. Дополнительная литература:

9. Федин Ф.О. Информационная безопасность [Электронный ресурс]: учебное пособие / Федин Ф.О., Офицеров В.П., Федин Ф.Ф.— Электрон. текстовые данные.— М.: Московский городской педагогический университет, 2011. — 260 c.— Режим доступа: http://www.iprbookshop.ru/26486.html.— ЭБС «IPRbooks»

6.3 Методические рекомендации по организации изучения дисциплины

Методически изучение дисциплины производится с применением активных форм проведения занятий. Принятая технология активного обучения базируется на работе, когда в процессе лекций и лабораторных работ, дополняемых самостоятельной работой обучаемых, выполняется серия проектно-исследовательских заданий и экспериментов, решение которых студентами позволяет практически применить полученные знания, развить необходимые общекультурные компетенции по данной дисциплине.

Успешное освоение дисциплины во многом зависит от самостоятельной работы студента. Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

Изучение конспекта лекции в тот же день, после лекции – 10-15 минут.

Изучение теоретического материала по учебнику и конспекту – 1 час в неделю в ходе подготовки к лабораторной работе.

Кроме чтения учебной литературы из обязательного списка рекомендуется активно использовать информационные ресурсы сети Интернет по изучаемой теме. Ответы на многие вопросы, связанные с темами дисциплины Вы можете получить в сети Интернет, посещая соответствующие информационные ресурсы.

Самостоятельное изучение тем учебной дисциплины способствует:

- закреплению знаний, умений и навыков, полученных в ходе аудиторных занятий;
- углублению и расширению знаний по отдельным вопросам и темам дисциплины;
- освоению умений прикладного и практического использования полученных знаний в области информационной безопасности.

Самостоятельная работа как вид учебной работы может использоваться на лекциях и лабораторных работах, а также иметь самостоятельное значение – внеаудиторная самостоятельная работа обучающихся – при подготовке к лекциям, лабораторным работам, к зачету.

Основными видами самостоятельной работы по дисциплине являются:

- самостоятельное изучение отдельных вопросов и тем дисциплины «Информационная безопасность»;
- выполнение лабораторного задания;
- оформление отчета по результатам лабораторных работ, подготовка к зачету.

Зачет показывает степень освоения дисциплины обучающимся.

При подготовке к зачету необходимо тщательно изучить лекционный материал, просмотреть все отчеты по лабораторным работам, чтобы еще раз осмыслить необходиммость теории в практических задачах. Целесообразно после изучения (по лекционному материалу и другим информационным источникам) конкретного вопроса из числа контрольных вопросов к зачету попытаться по памяти записать ответ на бумаге в возможно более развернутом виде. Это способствует развитию зрительной памяти и даст студенту больше уверенности в том, что он усвоид материал. Возникшие в ходе подготовки вопросы, на которые студент не смог найти ответа, необходимо записать и выяснить их на консультации у преподавателя.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Ресурсы информационно-телекоммуникационной сети «интернет». Обучающимся предоставлена возможность индивидуального доступа к следующим электронно-библиотечным системам.

1. Электронно-библиотечная система «Лань», режим доступа – с любого компьютера РГРТУ без пароля. – URL: https://e.lanbook.com/

2. Электронно-библиотечная система «IPRbooks», режим доступа – с любого компьютера РГРТУ без пароля, из сети интернет по паролю. – URL: https://iprbookshop.ru/.

3. Электронная библиотека ЮРАЙТ, режим доступа из сети интернет без пароля. – URL: https://biblio-online.ru/info/free-books/.

4. Электронный ресурс «Виртуальная кафедра АСУ» – https://rgrty.ru/.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

8.1. Операционная система Windows XP (Microsoft Imagine, номер подписки ID 700565239, бессрочно).

8.2 Пакеты программного обеспечения общего назначения (текстовые редакторы, графические редакторы, среды программирования и др.).

9 Материально-техническое обеспечение дисциплины

Для данной дисциплины применяется следующее материально-техническое обеспечение.

1. Лекционные занятия:

№	Наименование специальных помещений и помещений для самостоятельной работы	Перечень специализированного оборудования
1	Учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, № 254 главного учебного корпуса	1 проектор NEC NP 216 G, 1 экран, 1 компьютер Pentium G 620, маркерная доска, 32 ученических стола, 64 места Экран с ручным приводом – 1 шт. Доска маркерная 120х200 см Подключение к сети «Интернет» и обеспечение доступа в электронную информационно-образовательную среду РГРТУ.

2. Практические занятия и лабораторные работы:

Специализированный класс персональных ЭВМ (лаборатории 118, 127, 111а). Все компьютеры в классах подключены к локальной сети и имеют выход в «Интернет».

3. Прочее:

Рабочее место преподавателя, оснащенное компьютером с доступом в Интернет.